Bitcoin : une monnaie dématérialisée

Pascal Lafourcade, Jean-Guillaume Dumas

Bitcoin : une monnaie dématérialisée

Jean-Guillaume Dumas, Pascal Lafourcade, Patrick Redon

18 septembre 2019

Bitcoin (BTC) est une crypto-monnaie inventée par Satoshi Nakamoto en 2008 [1]. En 2016 plus de 100 000 transactions sont effectuées par jour [2]. Son originalité est que les transactions sont validées de manière totalement distribué entre les différents utlisateurs.

1 Principe

Bitcoin est une monnaie décentralisée utilisant des mécanismes cryptographiques. La particularité de cette monnaie est qu'elle ne nécessite pas de banque centrale pour émettre la monnaie ni pour gérer les transactions. Ainsi Bitcoin repose sur certains de ses membres, appelés *mineurs*, pour assurer la création de monnaie et la validation des transactions effectuées. Par construction, il n'y aura au maximum que 21 millions de bitcoins émis, et environ la moitié est en circulation à ce jour. La génération de nouveaux bitcoins et la validation de transactions reposent sur le concept de *preuve de travail*, ou *minage*, par analogie aux chercheurs d'or travaillant dans les mines. Ainsi pour valider les transactions courantes, il faut avoir résolu un calcul difficile : l'utilisateur qui réussit à faire ce travail est récompensé en bitcoins nouvellement créés.

La sécurité de ce système repose sur une architecture à clef publique : chaque utilisateur possède une clef publique (connue de tous) et une clef secréte (connue uniquement de son propriétaire). Ces clefs permettent à chaque utilisateur de signer électroniquement des transactions mais aussi à tout un chacun de pouvoir vérifier la validité de ces signatures.

2 Transactions

Chaque utilisateur possède un ou plusieurs compte(s) Bitcoin. Chaque compte correspond à une clef publique et contient des Bitcoins obtenus, soit lors de transactions avec d'autres utilisateurs, soit comme récompenses de minage. Pour dépenser des Bitcoins, il faut que l'utilisateur possède suffisamment de Bitcoins. Ensuite, l'intégratilité du contenu des pièces utilisées lors d'une transaction en Bitcoins doivent être utlisées. Ainsi, supposons qu'Alice possède dans son portefeuille 1, 2, 4, et 8 Bitcoins et qu'elle souhaite transférer $5,5$ Bitcoins à Bob. Elle peut utiliser, comme indiqué dans la Figure 1, ses deux "pièces" de 4 et 2 Bitcoins afin de transferer $5,5$ Bitcoins à Bob et $0,5$ Bitcoin à elle-même.

Dans la Figure 1, Alice souhaite faire une transaction de 12345 satoshis pour Bob [3]. Pour cela elle signe avec sa clef secrète l'empreinte de cette transaction et de toutes les précédentes transactions au monde. Pour que cette transaction soit valide et afin d'éviter la toute double dépense, il faut attendre que 6 blocs soient validés par des mineurs, ce qui correspond à environs une heure. Pour valider un bloc de nouvelles transactions, un mineur doit résoudre un objectif de hachage de la *block chain*. C'est-à-dire trouver une valeur aléatoire qui produira une empreinte commençant par un zéro de plus que le précédent objectif de hachage (ce qui demande une grande puissance de calcul). À l'heure actuelle l'objectif de hachage commence par plus de de $16 * 18$ zéros [4].

1. Un pseudonyme : https ://bitcoin.org/bitcoin.pdf
2. `https://blockchain.info/fr/charts/n-transactions`
3. 1 Bitcoin vaut cent millions de satoshis, la plus petite division d'un Bitcoin
4. Valeur du haché en hexadécimal $000000000000000037c4e9cc0b402cf92c20626eaf1ab67fa3478fc8134bf52$

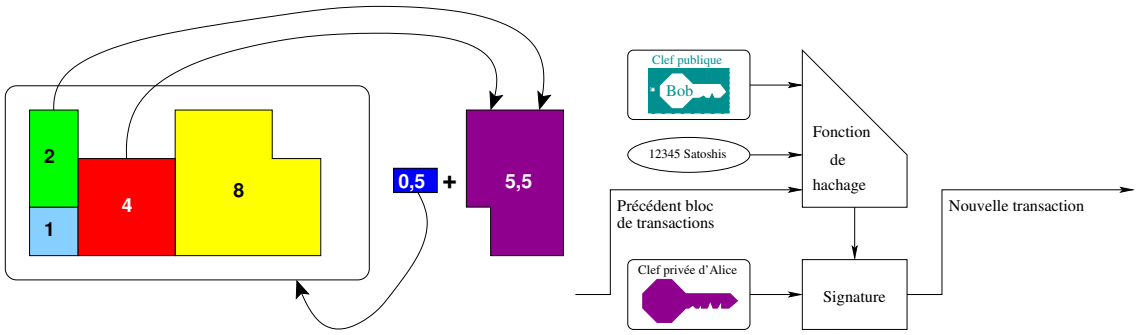

FIGURE 1 – Fonctionnement d'une transaction en Bitcoins, à gauche un portefeuille, à droite une partie de la chaîne.

3 Anonymat

Le modèle bancaire traditionnel garantit un certain degré d'anonymat en limitant l'accès aux informations de transactions aux seules parties intervenant dans la transaction et à leurs banques respectives. Au contraire, le modèle Bitcoin révèle publiquement toutes les transactions passées. Toutefois, une forme différente d'anonymat est préservée puisque l'identité des possesseurs des clefs publiques n'est pas nécessaire, seule une preuve de possession de la clef privée associée (la signature électronique de la transaction) est demandée. Le monde entier peut voir qu'un montant est transféré d'une clef publique à une autre, mais sans lien avec des personnes physiques ou morales. Cela ressemble au niveau d'information révélé par les bourses, quand les dates et tailles d'échanges individuels sont rendues publiques (le carnet d'ordres), mais sans révéler quelles étaient les parties impliquées.

Toutefois, pour Bitcoin, toutes les transactions d'une clef donnée sont liées, donc au moment où une personne entre ou sort du système Bitcoin (par exemple par un échange avec une autre monnaie) l'anonymat doit être levé, au moins auprès de l'organisme d'échange, et l'ensemble des transactions associées à cette clef peut alors être tracé.

4 Bitcoin un système monétaire

Le minage décentralisé, dans lequel n'importe quel agent économique peut créer un Bitcoin, et la circulation décentralisée du Bitcoin sur Internet, dans laquelle aucun acteur ne prélève de commission, a l'apparence du libéralisme économique. En réalité, le danger est que la décroissance des rendements implique que les fermes de minage doivent se concentrer afin de rester rentables. À partir du moment où quelques entités privées détiennent une majorité du marché de la certification des transactions en Bitcoin, elles détiennent en pratique la capacité d'émission monétaire et l'aspect distribué est perdu.

Références

[DLR15] Jean-Guillaume Dumas, Pascal Lafourcade, and Patrick Redon. *Architectures PKI et communications sécurisées.* Dunod, 2015.